Markets, M-21-9150
M. Nicolett

Research Note
26 March 2004

Magic Quadrant for IT Security Management, 1H04

The IT security management market is maturing and moving toward a common set of functional capabilities. Broad-scope software vendors provide integration benefits, while point solution vendors offer innovative technologies.

Core Topic
Security and Privacy: Security Infrastructure

Key Issue
What are the most-effective technologies and best practices to protect networks, systems, applications and data?

The IT security management market is driven by enterprises' needs to filter, aggregate and correlate security data from heterogeneous sources for real-time monitoring and historical analysis. Primary adopters of this technology tend to be large organizations with a complex IT infrastructure and dedicated IT security staff. Leaders are driving the market in terms of technical innovation, have rapidly growing production installed bases, and frequently are selected for and win competitive evaluations by organizations that make product-selection decisions based primarily on IT security management requirements.

Vendors gradually are converging on a common set of functional capabilities. Although there are areas of differentiation among leading vendors, differentiation is becoming difficult for customers to discern, short of a competitive trial. This convergence demonstrates a market that understands of customer requirements. It eventually will lead to pricing pressure and more-affordable software for enterprises. To avoid commoditization during the next three years, leading IT security management vendors will need to differentiate in areas such as:

- Ease of deployment
- Reduction in hardware deployment costs
- Monitoring and reporting for regulatory and audit compliance
- Integration of vulnerability management functions

IT security management technology providers include:

- Point solution vendors that have been the primary innovators and focus on the network security buying center (see "IT Security Management Point Solution Vendors, 1H04").

- Larger network and systems management (NSM) vendors that sell IT security management primarily to their customer bases, as well as a large security software vendor (see "IT Security Management Broad-Scope Software Vendors, 1H04").

Magic Quadrant Evaluation Criteria

The Magic Quadrant is a graphical portrayal of vendor performance in a market segment, based on viability, service/support, features and functionality, and technology.

Ability to Execute

An IT security management vendor's ability to execute indicates how well we expect it to perform. Key criteria include:

- Corporate commitment to market (for example, investment, marketing and executive focus)
- Customer (potential and current) knowledge and intimacy
- Price or cost
- Sales channel (direct and indirect)
- Marketing clarity and quality
- Influence on industry (for example, partners, standards and consumers)
- Management/organizational ability to support vision
- Customer references
- Overall corporate viability (financial, strategy and organization)
- Customer support

Completeness of Vision

A vendor's completeness of vision is how well its offerings match current and emerging market requirements. It also indicates how we expect the vendor to perform based on where the market is headed. Key criteria include:

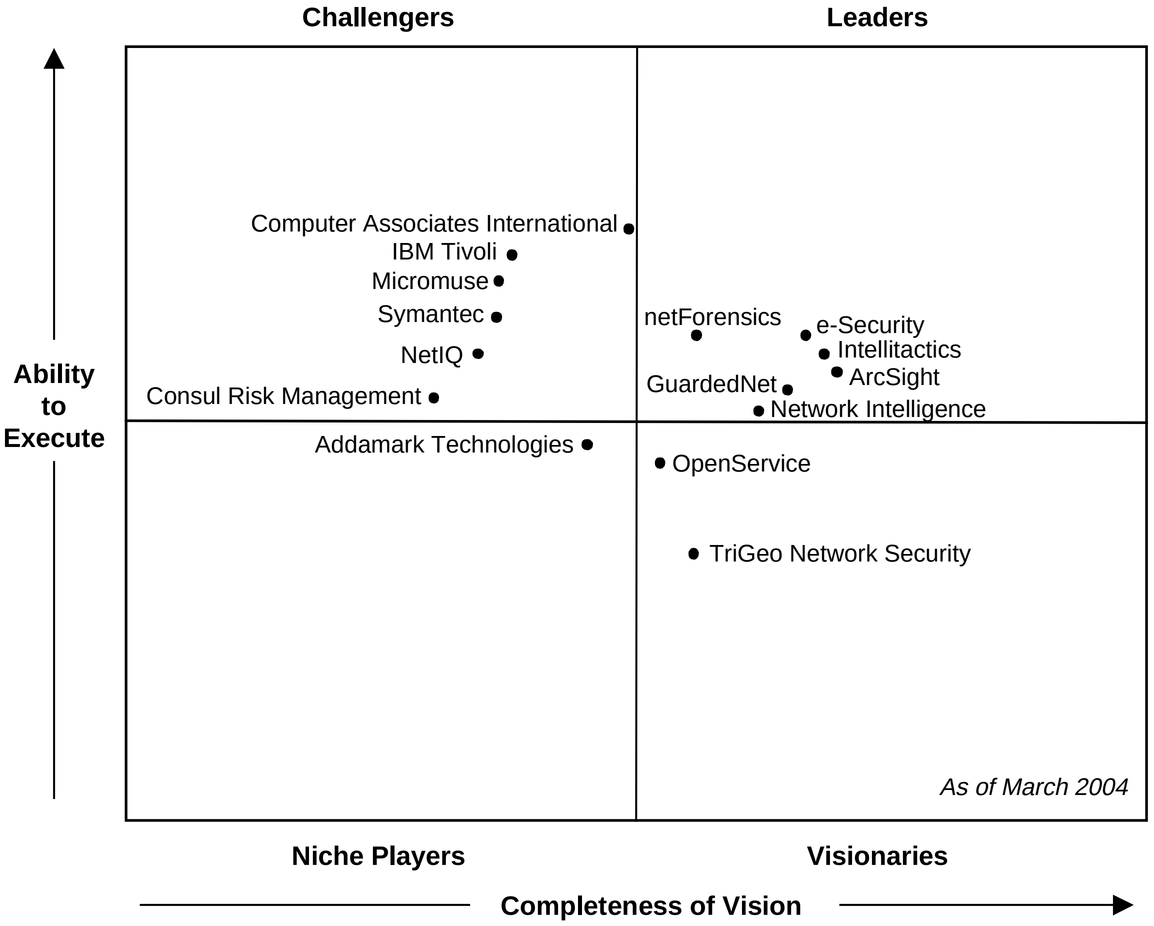
- Market understanding and knowledge
- Marketing strategy
- Sales strategy
- Offering strategy (for example, differentiation, features and functionality)
- Technology innovation

- Customer support/service account management vision

In evaluating features, functionality and technology, the ability to collect and correlate data from network security devices was heavily weighted, as was the integration of network threat information with server vulnerability assessment and policy compliance data (see "IT Security Management Technology Evaluation, 1H04").

The Magic Quadrant for IT Security Management, 1H04 (see Figure 1) offers an understanding of vendor positioning in the market and sets vendor performance expectations. Consider all quadrants when selecting a vendor. Appropriate vendors may be found in each of the quadrants, not only the Leaders quadrant. For example, some niche vendors provide unique technologies that solve critical IT security management issues.

Figure 1
Magic Quadrant for IT Security Management, 1H04



Source: Gartner Research (March 2004)

Leaders

Leaders frequently compete for business in large deployments where selection is based on product function and pre-sales support during pilots. These vendors have driven technology innovation in the market and are the most visible in client inquiries and references. e-Security, ArcSight and Intellitactics have been the most-visible competitors in large commercial and government technology evaluations, and have established large installed bases in these account types.

e-Security is an early provider of IT security management technology and has achieved a large installed base. It has proven its ability to stay ahead of the scalability needs of its largest corporate and government customers. e-Security has technology and sales relationships with Hewlett-Packard and the SAS Institute.

ArcSight has a smaller, but more-rapidly expanding, installed base than e-Security. It is a leader in functional areas such as vulnerability assessment data integration and visualization. ArcSight has introduced support for a compressed information store.

Intellitactics is selected by enterprise buyers who value configuration and integration flexibility over ease of deployment and ongoing maintenance. It is a leader in threat visualization and vulnerability assessment data integration, and incorporates a compressed information store.

netForensics has a large installed base and a long-standing, expanding relationship with Cisco Systems. This relationship provides netForensics with channel and customer access, unlike other point solution vendors. It also has made netForensics increasingly prevalent in Cisco's security initiatives. netForensics does not lead in IT security management technology areas, although it provides functionality that is "good enough" for the needs of many enterprises and the Cisco channel.

GuardedNet compares well with other leaders in terms of functionality and has a long-term focus on ease of deployment. Thus, GuardedNet provides more "out of the box" pre-defined functionality and less configuration flexibility than competitors such as e-Security, ArcSight and Intellitactics. GuardedNet has experienced rapid growth in its installed base and revenue, but it lags other leaders in terms of overall market visibility and installed base.

Network Intelligence has built a large installed base in midsize environments by providing an easy-to-deploy solution in appliance form that contains a compressed information store. Production deployment in large environments is driven by the recent introduction of cross-appliance consolidation capabilities and a full taxonomy. The taxonomy improves correlation capabilities that are not as well-developed as those of other leading vendors.

Visionaries

Visionaries provide solutions that meet many of the functional requirements of a market. Visionaries tend to lag leaders in areas such as product revenue, installed base and other execution factors. Visionaries include OpenService, a small NSM vendor that has changed its focus to security management, and TriGeo Network Security, a recent entrant that provides IT security management appliances.

OpenService is developing the capabilities of its Threat Manager offering. It is in the process of building out from its early-adopter installed base. Log aggregation capabilities are becoming available via integration with Addamark Technologies' Omnisight.

TriGeo Network Security's appliance is designed and priced for the small to midsize business market. Host agents can be directed by the appliance to implement blocking and other active responses to an incident. Customer feedback indicates a good match of pre-defined monitoring and reporting functions to customer requirements. TriGeo is establishing an installed base in a segment of the market that is not being served by leading software vendors.

Challengers

Most of the vendors in the Challengers quadrant are large NSM or security software vendors that have substantial sales, marketing and development resources. Many challengers sell IT security management solutions to their customers that value the potential integration of security management functions with other technologies from the vendor. They are not driving innovation in the market, and they rarely appear in competitive evaluations against leading vendors in Gartner's client or reference accounts that evaluate IT security management technology independently of the installed portfolio of products. Enterprises that use system management or security software of broad-scope IT security management vendors should consider the potential benefits of integration within that vendor's portfolio, as well as the potential of lower acquisition costs when the security management software is included in larger licensing agreements.

Of the NSM vendors, **IBM Tivoli** has been in the IT security management market the longest, and provides adequate, although not leading, technology. IBM Tivoli has succeeded in cases where customers value integration with IBM Tivoli technology.

In mid-2003, **Computer Associates International** announced general availability of its IT security management product. It has rapidly created a long list of supported devices and applications, including some vulnerability assessment products. Computer Associates also is integrating its vulnerability management and IT security management products. It is aggressively building out from a large beta program installed base, and it's products are installed in some very-large production environments.

Micromuse made good progress in 2003 in expanding its production installed base and further developing out-of-the-box security-oriented correlation and reporting. Micromuse has an original equipment manufacturer relationship with Cisco Systems to include its Netcool for Security Management product in the Cisco Info Center.

Symantec and **NetIQ** succeed in cases where the primary requirement is host log monitoring and analysis. However, they haven't been visible in competitive evaluations where the aggregation of high-volume security and network device information is a primary requirement. Symantec has a functionally complete IT security management solution, but it is building out from a small early-adopter installed base. During 2003, NetIQ focused on completing the integration of the technology from its PentaSafe acquisition.

Consul Risk Management provides unique capabilities in the area of activity log monitoring for security policy and regulatory compliance. It has a set of regulatory compliance monitoring modules. Consul's offering is limited in its real-time security event management functions.

Niche Players

Niche players satisfy a subset of the defined requirements for a market. They may be the best choice when there is a good match between the technology and a set of customer requirements. For example, Addamark Technologies focuses on providing technology for large-scale log data analytics.

Addamark Technologies is classified as niche because it provides a subset of the technology capabilities that this market generally requires. However, it provides capabilities that are unique and distinct from other vendors. The distinguishing characteristics of Addamark Omnisight are data compression and a focus on cost-effective, high-performance analytics against a large information store. Addamark's technology has been integrated with a number of other products in this market. Addamark Omnisight can collect and analyze data from firewalls, intrusion detection systems, network devices and server logs, but does not support real-time event data correlation and alerting.

Not on the Magic Quadrant

BindView is no longer being evaluated in this market because its technology primarily focuses on vulnerability management functions such as vulnerability assessment and security configuration policy compliance.

High Tower Software is a recent market entrant that has introduced appliance-based technology, which is being piloted by an initial set of customers.

Protego Networks is another recent market entrant that is building an early-adopter installed base. Protego differentiates its appliance with an automated incident-response capability that is implemented through dynamic configuration changes to switches, firewalls and routers.

Q1 Labs is in the early phases of a technology expansion that will add persistent event storage to its security-oriented network monitoring and correlation. However, it is not positioning its technology as an IT security management solution.

Bottom Line: When evaluating IT security management solutions, consider event management and data analysis requirements for the enterprise's perimeter, servers and applications. Appliances can reduce deployment costs. Solutions with compressed information stores support data retention for regulatory compliance. Products from broad-scope vendors provide integration with management infrastructure, while leading point solution vendors offer the most-complete IT security management functionalities.